REMARKS

Claims 1-12 are pending in this application.

Rejections of claims 1-5, 8, and 10-11 under 35 U.S.C. 102(e)

Claims 1-5, 8, and 10-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Linnartz (U.S. Patent No. 6,314,518).

Applicants respectfully submit that in the Office Action Summary sheet, attached in front of the Office Action, only claims 1, 3-5 and 7-11 are rejected and claims 2, 6 and 12 are objected to. However, page 4 of the Office Action states that "Claims 1-5, 8 and 10-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Linnartz (US 6,314,518)." There is no discussion of claim 2 in the body of the U.S.C. 102(e) rejection and claim 2 is identified as being objected to in the Office Action Summary, and is identified as Allowable in the discussion on page 8 of the Office Action under the heading "Allowable Subject Matter." Therefore, as claim 2 is identified as only being objected to, as stated in the Office Action Summary, and is allowable if rewritten to include all of the limitations of the base claim (*see* page 8 of the Office Action), Applicants respectfully submit that claim 2 is not rejected under 35 U.S.C. 102(e). Thus, Applicants respectfully submit that only claims 1, 3-5, 8 and 10-11 should be rejected under 35 U.S.C. 102(e) on page 4 of the Office Action.

The present claimed arrangement provides a method of protection against the copying of digital data stored on a storage medium. The method includes identifying whether the digital data are encrypted and whether the digital data are watermarked. One of a permission and prohibition to copy and/or to play the digital data are delivered as a function of an identification of an encryption of the digital data and a watermarking of the digital data.

In the claimed arrangement, a storage medium containing data is checked (examined) to determine whether the digital data contents can be played back (e.g. for video data, it is checked whether the video data can be displayed on a screen) or can be copied (i.e. duplicated in another storage medium) or on the contrary, if the data cannot be played back or cannot be copied. This is determined by identifying whether the digital data are encrypted

and watermarked. The permission or prohibition to copy are delivered based on the identification of the encryption and watermarking.

Linnartz describes a system for copy protecting content information. Copy protecting content information has an arrangement for receiving and controlling the playback of encoded video. The video content, e.g. MPEG compressed digital video, is watermarked and includes a control signal indicating the status (e.g. playback only, one generation of copy allowed, etc). In the receiver device, a check is performed to allow playback dependent on the watermark. The watermark is extracted in a separate decoder device, such as an external MPEG decoder. The receiver device starts the playback via the external decoder, and the separate decoder communicates retrieved watermark information via a link to the playback device. The playback device checks the watermark information against further supplemental information, such as a physical mark on the record carrier or the control signal. The communication may be protected by cryptographic methods, such as a digital signature (*see* Abstract).

As admitted by the Office Action dated March 19, 2007, Linnartz does not show or suggest encrypted digital data (*see* page 2: "Applicant argues that Linnartz does not teach identifying whether said digital data are encrypted. This is true" and page 4: "Linnartz does not explicitly disclose identifying whether said digital data are encrypted and delivering one of a permission and prohibition to copy and/or to play said digital data as a function of an identification of an encryption of digital data."). However, the current Office Action dated December 13, 2007 argues that that "upon further consideration of claim 1, the examiner believes that it could be rejected based on Linnartz's teachings alone." Applicants respectfully disagree.

Linnartz, neither discloses nor suggests "identifying whether said **digital data are encrypted**" or "delivering one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: - **an encryption** of said digital data; **and** - a watermarking of said digital data" as recited in the present claimed arrangement. The Office Action on page 4 cites col. 7, lines 64-67 of Linnartz as "identifying whether said digital data

are encrypted." Applicants respectfully disagree. The cited passage merely describes that "[r]ecorders may accept content **without detecting the watermark itself**, if the content plus a cleartext version of the watermark bits are signed by a compliant and authorized device (e.g. an MPEG encoder)" (col. 7, lines 64-67). This is wholly unlike the present claimed arrangement which delivers "one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: - **an encryption of said digital data; and - a watermarking of said digital data**" as recited in claim 1. Unlike the present claimed arrangement, Linnartz does not base "delivering one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: - an encryption of said digital data; **and** - a watermarking of said digital data." Rather, Linnartz merely describes that if the content and cleartext version of the watermark bits are signed by a trusted device (e.g. an MPEG encoder), then a recorder will accept the content without detection of the watermark. Moreover, it follows from the cited passage that any possible encryption scheme that may be utilized by the recorder to establish trust (i.e. a one way cryptographic algorithm, as suggested by the Office Action on page 4) in Linnartz would merely be used as a method of verifying that a compliant and authorized device signed the watermark. Thus, any encryption in Linnartz is merely used as a watermark check (*see* col. 9, lines 8-22). This is completely unrelated to and does not disclose or suggest "identifying whether said digital data are encrypted ... delivering one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: - **an encryption of said digital data**; and - a watermarking of said digital data" as recited in claim 1 of the present arrangement.

The Office Action further argues that "[s]igning the digital content means that a one way cryptographic algorithm was applied to the content. Identifying whether or not a signature of the content exists means identifying whether the digital content was encrypted, i.e. processed using the one way cryptographic hash algorithm." Applicants respectfully submit that the digital signature in Linnartz is completely unlike "delivering one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: - an encryption of said digital data; and - a watermarking of said digital data" as recited in claim 1 of the present arrangement. Additionally, Linnartz describes that

the recording drive "hashes ... and signs the MPEG stream using well known cryptographic algorithms like RSA or DSA. The MPEG decoder then verifies the signature, detects the watermark and send[s] a message back to the drive. This message contains the retrieved watermark bits concatenated to the random number and the signature as it was placed by the drive, and MPEG decoder signs this message again" (col. 8, line 65-col. 9, line 4). Alternatively, "the burden of checking hashes is not placed with the drive or with the decoder, but instead is performed by the MPEG encoder. The compliant MPEG encoder already pre-computes a set of values, which it provides to the recorder and the drive" (col. 9, lines 12-16). Thus, the digital signature used by Linnartz is for verification of the MPEG stream by the MPEG decoder. This is completely unlike and unrelated to "delivering one of a **permission and a prohibition to copy and/or to play said digital data**" as recited in claim 1 of the present arrangement.

Furthermore, the Office Action on page 5 argues that "Linnartz further discloses delivering a permission for digital copying when: an encryption of said digital data has not been identified; and a watermarking of said digital data has not been identified (col. 5, lines 1-10). The cited portion discloses that content, if it lacks a watermark is considered to be in state d, a free copy state. There being no watermark means that the watermark has not been identified and the data being in a free copy state means a copy permission is delivered **whether or not encryption of digital data is identified.**" Applicants respectfully submit that the cited passage merely describes the different states which watermarks may correspond to (i.e. states a, b, c and d-free copy, no watermark state). However, Linnartz does not deliver "one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: - an encryption of said digital data; **and** - a watermarking of said digital data." Not having a watermark present, as in Linnartz may allow a user to make copies of the disc. However, this is wholly unlike the present claimed arrangement in which "a permission and a prohibition to copy and/or to play said digital data" is dependent upon "a function of an identification of: - an encryption of said digital data; **and** - a watermarking of said digital data" as recited in claim 1 of the present invention. Therefore, as Linnartz allows copying of a digital disc irrespective of encryption of digital data, Linnartz neither discloses nor suggests "delivering one of a permission and a prohibition to copy and/or to play said digital data as a

function of an identification of: - an encryption of said digital data; and - a watermarking of said digital data" as recited in claim 1 of the present arrangement.

Moreover, Linnartz describes a system for transferring content information and supplemental information related thereto. The supplemental information includes a control pattern which is applied to a one-way function to generate a watermark. The control pattern and watermark form a cryptographically controlled counter. The "cryptographic counter ... can be decremented but not incremented" (col. 5, lines 58-59). The counter is decreased in the player before the processed control pattern is provided to a recorder thereby allowing a limited number of generations of copies to be produced. As soon as the counter is decreased to a point where no further copies are allowed, the pattern will no longer match the watermark and reproduction will be blocked. Should the watermark or control pattern be altered or manipulated, the quality of the reproduced content will be severely degraded. The present claimed arrangement recognizes and solves the problems with systems such as Linnartz's (*see* Specification, page 3, lines 3-25). For example, the system of Linnartz "does not by itself make it possible to prevent copying by an analog route" (Specification, page 3, lines 23-25). Therefore, the present claimed arrangement provides a more secure way to permit and prohibit copying and/or playing of the digital media containing the digital data by "delivering one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: - **an encryption** of said digital data; **and - a watermarking** of said digital data." Such is neither disclosed nor suggested by Linnartz. Thus, the system of Linnartz does not disclose or suggest "delivering one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: - an encryption of said digital data; and - a watermarking of said digital data" as recited in claim 1 of the present arrangement. Consequently, it is respectfully requested that the rejection of claim 1 under 35 U.S.C. 102(e) should be withdrawn.

Claim 4 is dependent on claim 1 and is allowable for the reasons presented above with respect to claim 1. Claim 4 is also not anticipated by Linnartz because Linnartz neither discloses nor suggests "delivering a prohibition of playing of said digital data when: - an

encryption of said digital data has not been identified; and - a watermarking of said digital data has been identified" as recited in claim 4 of the present arrangement.

Applicants respectfully submit that the current Office Action dated December 13, 2007 may have contained a typographical error with respect to the cited passage "col. 4, lines 30-47" of Linnartz. Applicants believe the current Office Action should have cited "col. 5, lines 30-47" of Linnartz, as on page 6 of the previous Office Action dated March 19, 2007. Applicants will discuss both passages, currently cited col. 4, lines 30-47 and previously cited col. 5, lines 30-47.

Cited col. 4, lines 30-47 merely describes:

> "For a casual copier it is impossible to insert the physical mark of RO content on a recordable disc, even if he happens to know the bit content of the physical marker. It should also be recognized that small-scale piracy will be attempted, using read-only disc-pressing equipment. This is already a common method used for large and small scale pirating of audio CDs and CD ROM's. It becomes economically attractive to publish on (silver) CD RO instead of (golden) CD Recordable, if the size of the order is above about a few hundred discs ... Similar attacks with DVD read-only is not adequately countered if the detector in consumer players only check for recordable and read-only media, without checking the relation between the origin of the read-only medium and its content. For a small scale pirate who wants to order a publishing house to press a certain quantity of discs, it is technically difficult to find the bit value of the physical marker" (col. 4, lines 30-48).

Thus, Linnartz in the cited passage merely describes that it is impossible to insert the physical mark of RO (read-only) content on a disc. Therefore, small-scale piracy is attempted using read-only disc-pressing equipment. Publishing on silver CD RO instead of golden CD Recordable media is economically attractive in large scale. The small scale pirates are already pirating through RO. Similarly, attacks with DVD read-only are not countered if the detector in the consumer players only checks for recordable and read-only media, without checking the relationship between the origin of the read-only medium and its content. However, nowhere in this cited passage or elsewhere in Linnartz is there suggestion or disclosure of "delivering a **prohibition of playing** of said digital data when: - **an encryption**

of said digital data has not been identified; and - a watermarking of said digital data has been identified" as recited in claim 4 of the present arrangement.

Previously cited col. 5, lines 30-47 does not anticipate the features of the claimed arrangement. Specifically, col. 5, lines 30-47 describes:

> "Subsequent detection by the above control systems would prevent recording and allow playback ... An original record carrier containing video or audio is played back in a playback system 41. A recordable media 43, such as an optical disc 44 or a tape 45, is recorded in recording drive system 42. The recording drive system 42 records only, if the 'one-copy' state is detected, and then also the state is modified to 'no-more-copy' on the recordable media. The basic record control is designed to prevent a casual consumer from copying 'never-copy' and 'no-more-copy' material onto a recording device. The recording device would detect the watermark and inhibit copy of the content, if 'Never-copy' or 'No-more-copy' state is detected. The modified state is passed on the recordable carrier as a new ticket T. The ticket contains multiple validation tokens. During each playback and recording step, one token is removed" (col. 5, lines 30-48).

The cited passage describes recording onto a disc in a recording drive system only if a proper state is detected. When the state is modified to "no-more-copy," no more copies can be recorded. However, nowhere in this cited passage or elsewhere in Linnartz is there any suggestion or disclosure of "delivering a **prohibition of playing** of said digital data when: - **an encryption of said digital data has not been identified**; and - a watermarking of said digital data has been identified" as recited in claim 4 of the present arrangement. Therefore, Linnartz does not anticipate the features of claim 4 of the present arrangement. Consequently, it is respectfully requested that the rejection of claim 4 under 35 U.S.C. 102(e) should be withdrawn.

Claims 5, 8, 10 and 11 are dependent on claim 1 and therefore are also considered patentable for the reasons presented above with respect to claim 1. Consequently, it is respectfully requested that the rejection of claims 5, 8, 10 and 11 under 35 U.S.C. 102(e) be withdrawn.

In view of the above remarks it is respectfully submitted that Linnartz does not anticipate the features of the present claimed arrangement. It is thus, further respectfully submitted that this rejection is satisfied and should be withdrawn.

Rejection of claim 7 under 35 U.S.C. 103(a)

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Linnartz (U.S. Patent No. 6,314,518) in view of Ichinoi (U.S. Patent No. 6,266,477).

Ichinoi describes a data signal recording and playback method and system that can determine whether the recording medium being used is a high-performance recording medium for recording and playing back both digital and analog signals, or a standard-performance medium, and selecting its recording specifications accordingly. When recording/playing back digital data signals and analog data signals received as inputs to the system, if a high-performance magnetic tape is identified, the system selects for recording, one of the three input signals: a digital data signal, an analog data signal obtained through D/A conversion of a digital data signal, or an analog data signal input as such. If the recording medium being used is a standard-performance magnetic tape, the system selects for recording, either an analog data signal obtained through D/A conversion of a digital data signal, or an analog data signal input as such (*see* Abstract).

Ichinoi, similar to Linnartz, neither discloses nor suggests "[a] method of protection against the copying of digital data stored on a storage medium, said method comprising: identifying whether said digital data are encrypted" or "delivering one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: - an encryption of said digital data; and - a watermarking of said digital data" as recited in claim 1 of the present arrangement. Ichinoi describes "a data signal recording and playback system that is capable of performing a variety of output switching functions, including the conversion of digital signals to analog signals prior to output. More specifically ... [Ichinoi] provides a data signal recording and playback system wherein all required output switching is performed within the recording and playback system itself" (col. 2, lines 26-33). Therefore, Ichinoi (with Linnartz) is completely unrelated to the present claimed arrangement and does

not disclose or suggest "[a] method of **protection against the copying of digital data** stored on a storage medium, said method comprising: identifying whether said digital data are encrypted" or "delivering one of a **permission and a prohibition to copy and/or to play** said digital data as a function of an identification of: - an encryption of said digital data; and - a watermarking of said digital data" as recited in claim 1 of the present arrangement.

Furthermore, even if the system of Linnartz and Ichinoi were combined, as suggested by the Office Action, the combination would not make the present claimed arrangement unpatentable. The combined system would produce a disc recording and playback system. The system would read the watermark included on the disc being read and depending upon the state of the watermark, the recording system would determine if copies of the disc can be made or not. The combined system would further include a digital recording system to record and playback digital or analog signal data. The combined system of Linnartz and Ichinoi, similar to individual systems, would not disclose or suggest "delivering one of a permission and a prohibition to copy and/or to play said digital data as a function of an identification of: - an encryption of said digital data; and - a watermarking of said digital data" as recited in claim 1 of the present arrangement. As claim 7 is dependent on claim 1, claim 7 is also allowable over Linnartz and Ichinoi for the same reasons as claim 1 discussed above. Consequently, it is respectfully requested that the rejection of claim 7 under 35 U.S.C. 103(a) should be withdrawn.

In view of the above remarks, it is respectfully submitted that Linnartz and Ichinoi, when taken alone or in combination do not make the present claimed arrangement unpatentable. It is thus further respectfully submitted that this rejection is satisfied and should be withdrawn.

Claim 9 is allowed. Additionally, claims 2, 6 and 12 are indicated as allowable if rewritten to include all the limitations of the base claim and any intervening claims. Applicants respectfully submit that, in view of the above remarks, claim 1 is patentable over Linnartz. Therefore, as claims 2-8 and 10-12 are dependent upon claim 1, these claims are

likewise patentable over Linnartz and Ichinoi. Therefore, in view of the above remarks, applicants respectfully submit that all pending claims are in condition for allowance.

Having fully addressed the Examiner's rejections, it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at the phone number below, so that a mutually convenient date and time for a telephonic interview may be scheduled.

No additional fee is believed due. However, if an additional fee is due, please charge the additional fee to Deposit Account 07-0832.

Respectfully submitted,
Sylvain Chevreau et al.

By: _____
Jack Schwartz
Reg. No. 34,721
Tel. No. (609)734-6866

Thomson Licensing, LLC
Patent Operations
PO Box 5312
Princeton, NJ 08543-5312
June 11, 2008